

## PRUEBA DE HABILIDADES PRÁCTICAS

ARMANDO VILLA MARENGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE SISTEMAS  
VALLEDUPAR  
2018

PRUEBA DE HABILIDADES PRÁCTICAS

ARMANDO VILLA MARENGO

TUTOR:  
GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE SISTEMAS  
VALLEDUPAR  
2018

## INTRODUCCION

Mediante el desarrollo del presente TRABAJO buscamos realizar la implementación de la red corporativa para la empresa de TECNOLOGÍA la cual le va a brindar la posibilidad de crecer a pasos agigantados gracias a su excelente servicio y fiabilidad que este presta a todos sus clientes. Esperamos ser un punto de apoyo para la misma y una fortaleza para su futuro y su crecimiento a nivel local y nacional.

Es importante poder ayudar, pero al igual en el punto que nos encontramos, el desarrollo de esta propuesta también va a ser excelente para nuestra formación profesional, pues gracias a esta propuesta podremos practicar lo aprendido hasta el momento y que mejor manera que desarrollando directamente sobre un caso real que pueda exigirnos a cada día mejorara más.

La propuesta como vemos el archivo entregado donde los plasman el ejercicio será desarrollada desde cero, no hay nada de esta red sobre lo cual podamos trabajar, debemos analizar la situación actual de la empresa para poder tomar decisiones al respecto. Todo el diseño y el montaje lo realizaremos bajo dispositivos CISCO.

Espero el trabajo sea del agrado de todos ustedes y que les contribuya igualmente a solucionar algunas dudas que en el momento tenga.

El proyecto nos va a favorecer muchísimo puesto que será la forma de que apliquemos todo ese conocimiento que a lo largo del Diplomado hemos adquirido, queremos generar en nosotros esa confianza que necesitamos para poder abordar proyectos de cualquier dificultad.

Las redes han cambiado de forma significativa nuestra forma de vivir, nuestra forma de relacionarnos. Estas nos han permitido realizar muchas cosas que antes pensábamos imposibles pero que ahora las tenemos y las podemos hacer con gran facilidad. Utilizamos la red de distintas formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y mucho más.

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Desarrollo e implementación de la red de datos para la empresa de TECNOLOGIA.

Diseño de la Topología de la empresa de TECNOLOGIA, la cual tiene una serie de sedes a nivel de diferentes ciudades, siguiendo una serie de pautas y necesidades que se nos establece dentro del documento.

### **OBJETIVOS ESPECÍFICOS**

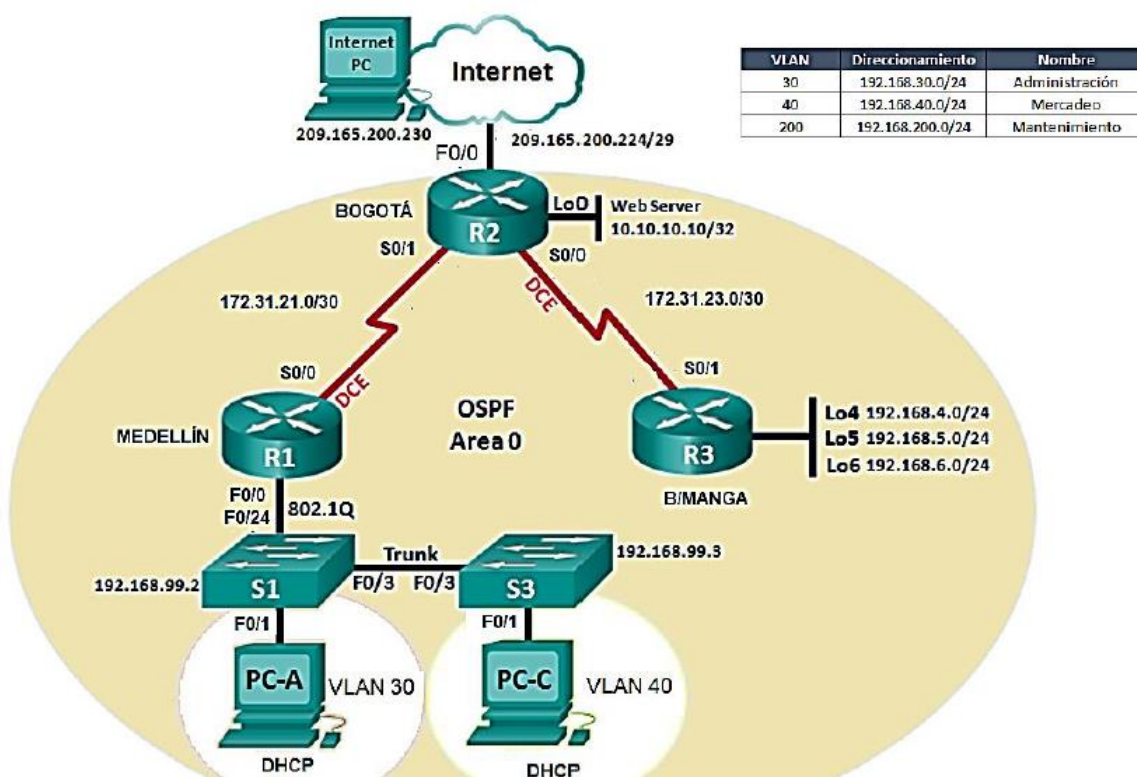
- Diseñar la red de datos para la empresa la cual se ajuste a las necesidades reales de la empresa.
- Practicar todo lo aprendido hasta el momento, lo cual nos genere esta confianza que necesitamos para el desarrollo de este tipo de propuesta.
- Aplicaremos VLSM en todo el diseño de la red, la intención es mitigar el desperdicio de direcciones IP.
- Realizar la documentación general de la red.
- Practicarnos en la configuración de protocolos de enrutamiento, reconociendo las posibilidades de cada uno de ellos.
- Comprender mucho mejor la utilización de los diferentes comandos de configuración.

## DESCRIPCIÓN DEL ESCENARIO PROPUESTO PARA LA PRUEBA DE HABILIDADES

**Escenario:** Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

### Topología de red

#### Topología de red



1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

#### OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

#### Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
  - Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
  - Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
  4. En el Switch 3 deshabilitar DNS lookup
  5. Asignar direcciones IP a los Switches acorde a los lineamientos.
  6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
  7. Implement DHCP and NAT for IPv4
  8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
  9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.



## DESARROLLO DE LA GUÍA.

Examen de ENTRENAMIENTO.

Debemos poner un servidor WEB, pues Packet Tracer no lo admite como comando, debemos ponerlo de manera real.

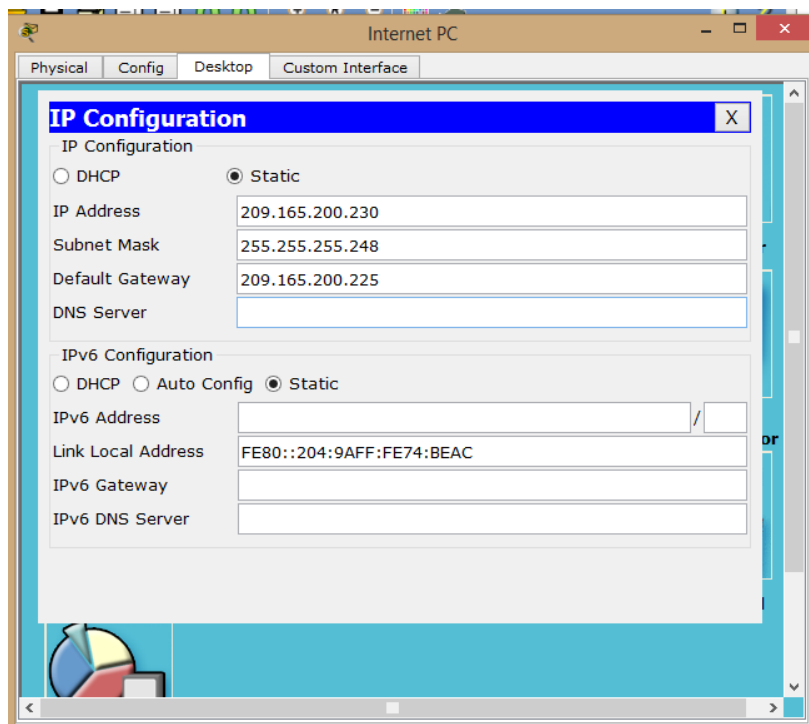
- Debemos borrar la configuración de los dispositivos switches.
  - Erase start-up config
- Borra a base de datos de las VLAN.
  - Delete vlan.dat
- Reiniciamos
  - Reload.

## CONFIGURAMOS LA IP INTERNET.

IP: 209.165.200.230

Mask: 255.255.255.248

Gateway: 209.165.200.225

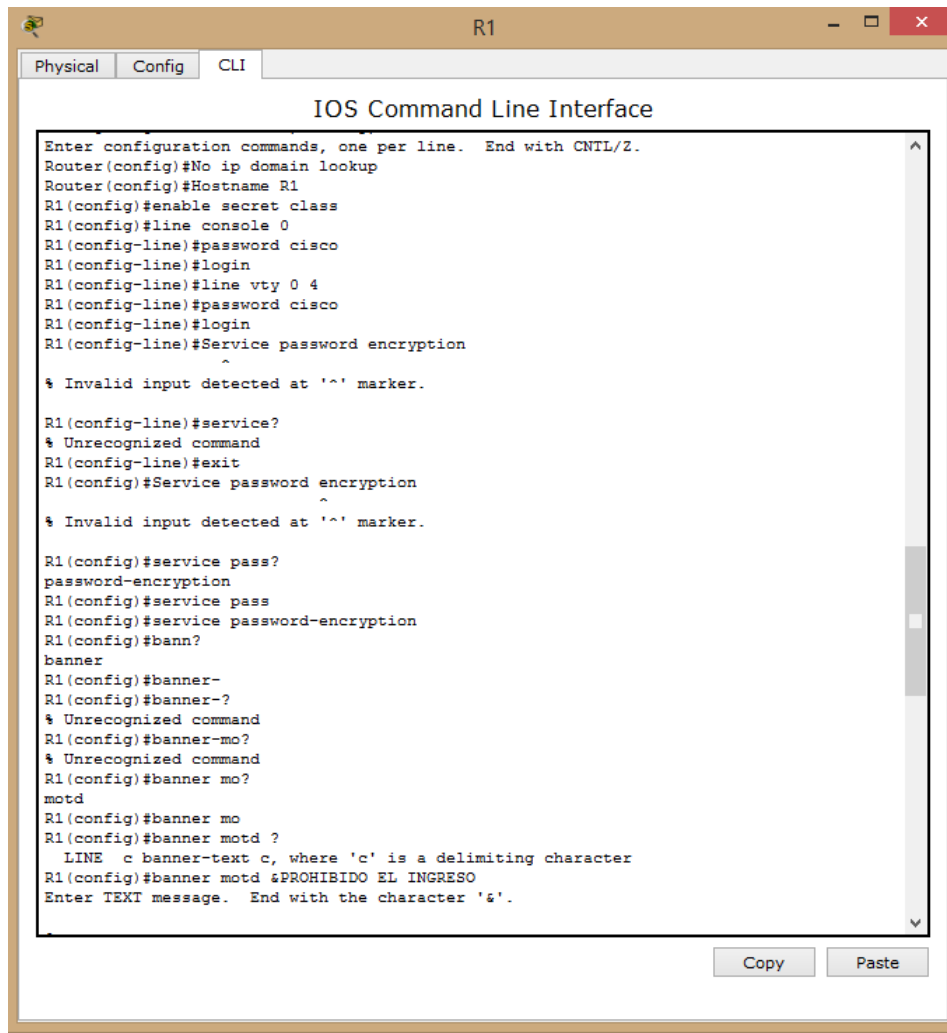


## Configuramos R1.

No ip domain lookup

Hostname R1

Enable secret class  
Line console 0  
    Password cisco  
    Login  
Line vty 0 4  
    Password class  
    Login  
Service password encryption  
  
Banner motd &PROHIBIDO EL INGRESO.

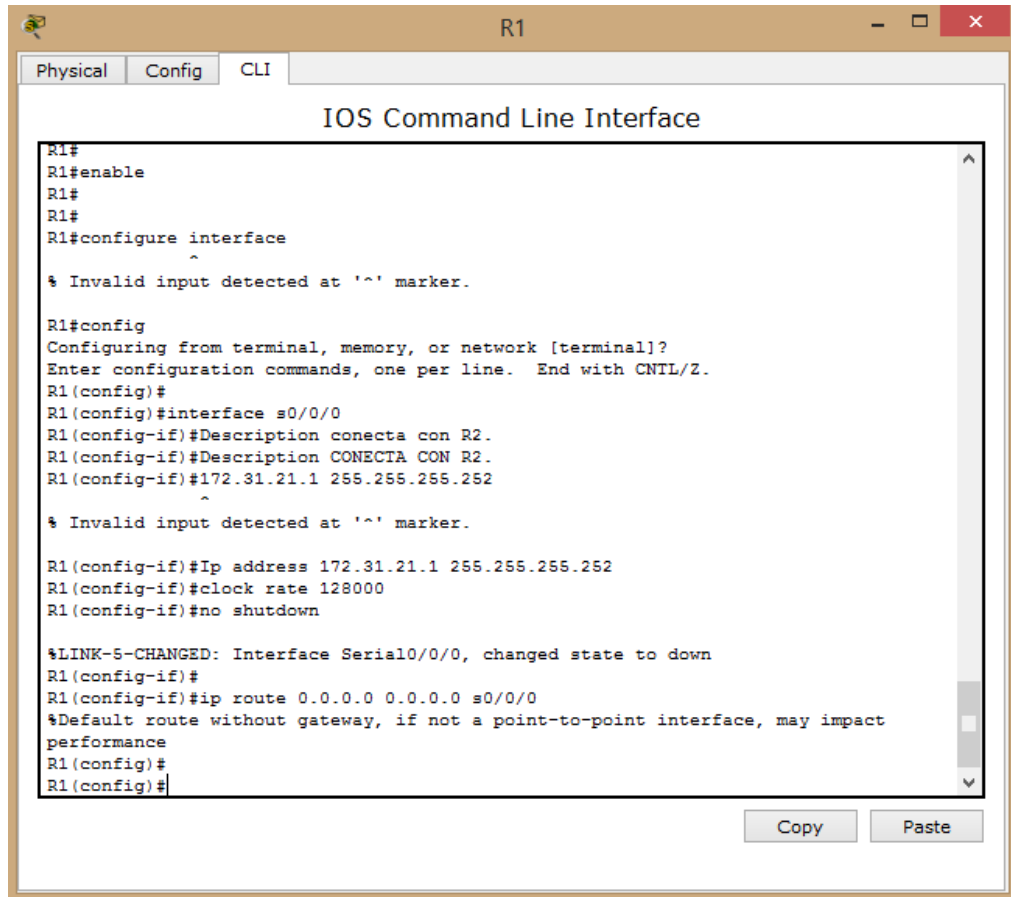


```
R1
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#No ip domain lookup
Router(config)#Hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#Service password encryption
^
% Invalid input detected at '^' marker.
R1(config-line)#service?
% Unrecognized command
R1(config-line)#exit
R1(config)#Service password encryption
^
% Invalid input detected at '^' marker.
R1(config)#service pass?
password-encryption
R1(config)#service pass
R1(config)#service password-encryption
R1(config)#bann?
banner
R1(config)#banner-
R1(config)#banner-?
% Unrecognized command
R1(config)#banner-mo?
% Unrecognized command
R1(config)#banner mo?
motd
R1(config)#banner mo
R1(config)#banner motd ?
LINE c banner-text c, where 'c' is a delimiting character
R1(config)#banner motd &PROHIBIDO EL INGRESO
Enter TEXT message. End with the character '^'.
Copy Paste
```

Configure interface s0/0/0  
Description CONECTA CON R2.  
Ip address 172.31.21.1 255.255.255.252  
Clock rate 128000  
No shutdown

- Configuramos una ruta por defecto

ip route 0.0.0.0 0.0.0.0 s0/0/0



```
R1#
R1#enable
R1#
R1#
R1#configure interface
^
% Invalid input detected at '^' marker.

R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#interface s0/0/0
R1(config-if)#Description conecta con R2.
R1(config-if)#Description CONECTA CON R2.
R1(config-if)#172.31.21.1 255.255.255.252
^
% Invalid input detected at '^' marker.

R1(config-if)#Ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#
R1(config)#
```

### • Configuramos R2.

No ip domain-lookup

Hostname R2

Enable secret class

Line console 0

    Password cisco

    Login

Line vty 0 4

    Password cisco

    Login

Service password-encryption

Ip http server "comando no soportado por PACKET TRACER"  
Banner motd & PROHIBIDO EL ACCESO

Interface s0/0/1  
Description CONEXION CON R1  
Ip address 172.31.21.2 255.255.255.252  
no shutdown

interface s0/0/0  
description CONEXION CON R3  
ip address 172.31.23.1 255.255.255.252  
clock rate 128000  
no shutdown

interface g0/1 "es la simulación de INTERNET"  
description CONEXION A INTERNET  
ip address 209.165.200.225 255.255.255.248  
no shutdown

- como siguiente paso debemos configurara el servidores WEB

interface g0/0  
ip address 10.10.10.1 255.255.255.0  
no shutdown  
description CONEXIÓN CON WEB SERVER

- configuramos el servidor web

ip address 10.10.10.10  
mask: 255.255.255.0  
Gateway: 10.10.10.1

- configuramos una ruta por defecto

ip route 0.0.0.0 0.0.0.0 g0/1 "que salga hacia internet.

- Configuramos el ROUTER 3.

No ip domain-lookup  
Hostname R3

```
Enable secret class
Line console 0
    Password cisco
    login
Line vty 0 4
    Password cisco
    Login
Service password-encryption
Banner motd & PROHIBIDO EL INGRESO
```

```
Interface s0/0/1
Description CONEXIÓN CON R2
Ip address 172.31.23.2 255.255.255.252
No shutdown
```

- Vamos a crear las interfaces loopback

```
Interface loopback 4
Ip address 192.168.4.1 255.255.255.0
No shutdown
```

```
Interface loopback 5
Ip address 192.168.5.1 255.255.255.0
No shutdown
```

```
Interface loopback 6
Ip address 192.168.6.1 255.255.255.0
No shutdown
```

- Configurar ruta por defecto por serial 1

```
Ip route 0.0.0.0 0.0.0.0 s0/0/1
```

- Configuramos switch 1

```
No ip domain-lookup
hostname S1
enable secret class
line console 0
    password cisco
    login
line vty 0 4
    password cisco
    login
```

```
service password-encryption
banner motd & PROHIBIDO EL INGRESO
```

- **Configuramos switch 3**

```
No ip domain-lookup
hostname S3
enable secret class
line console 0
    password cisco
    login
line vty 0 4
    password cisco
    login
service password-encryption
banner motd & prohibido ingreso
```

- En este punto debemos verificar la conectividad de los dispositivos.

**Step 7: Verify network connectivity.**

Use the **ping** command to test connectivity between network devices.

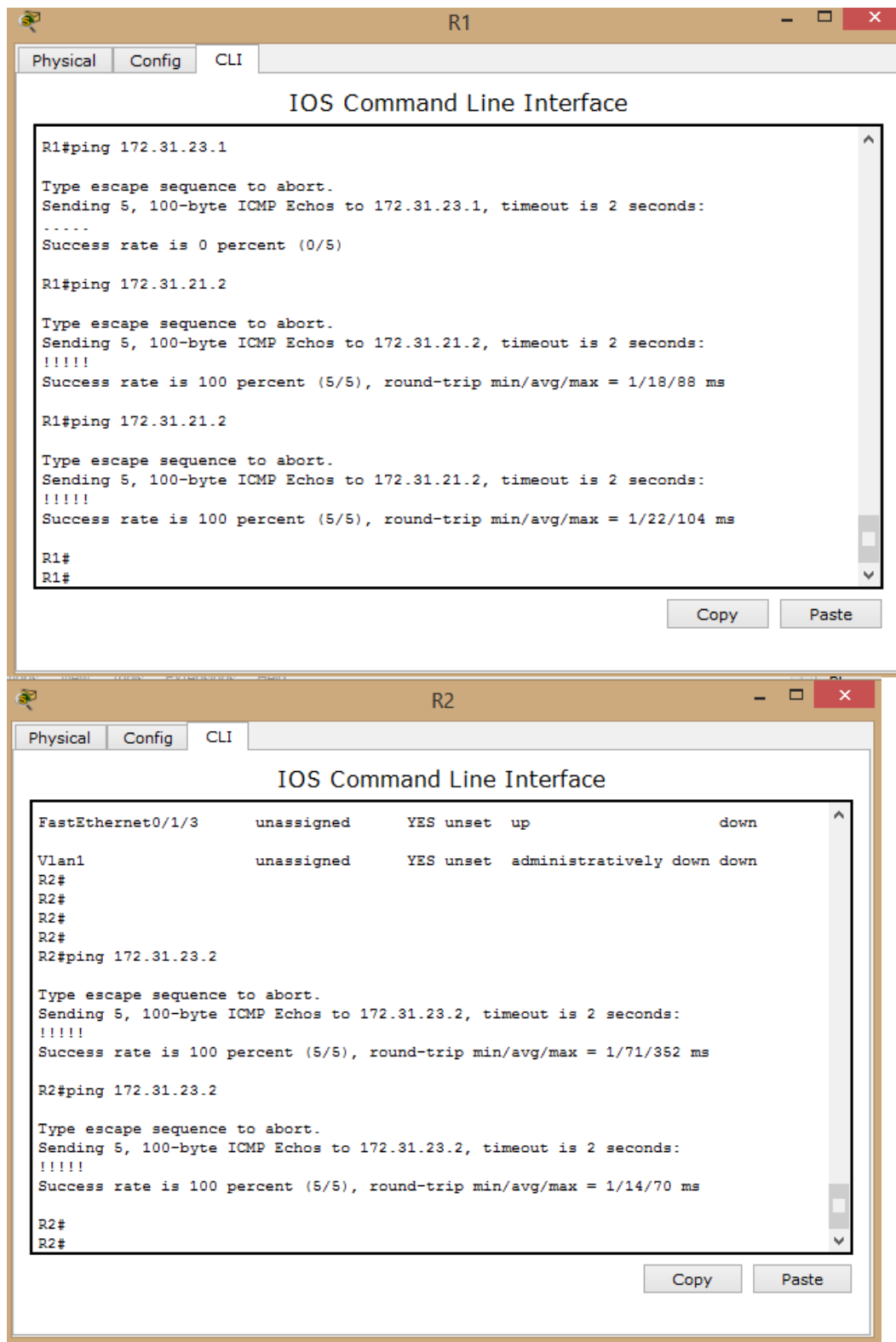
Use the following table to methodically verify connectivity with each network device. Take c establish connectivity if a test fails:

From	To	IP Address	Ping Results
R1	R2, S0/0/0		
R2	R3, S0/0/1		
Internet PC	Default Gateway		

**Note:** It may be necessary to disable the PC firewall for pings to be successful.

**Instructor Sign-off Part 2:** \_\_\_\_\_

**Points:** \_\_\_\_\_ of **28**



Todos los PING son satisfactorios, con lo cual se verifica la correcta configuración

de cada una de las INTERFACES.

- Configuramos la seguridad, las VLANS y el ruteo entre las VLANS

- Iniciamos con el SWITCH 1

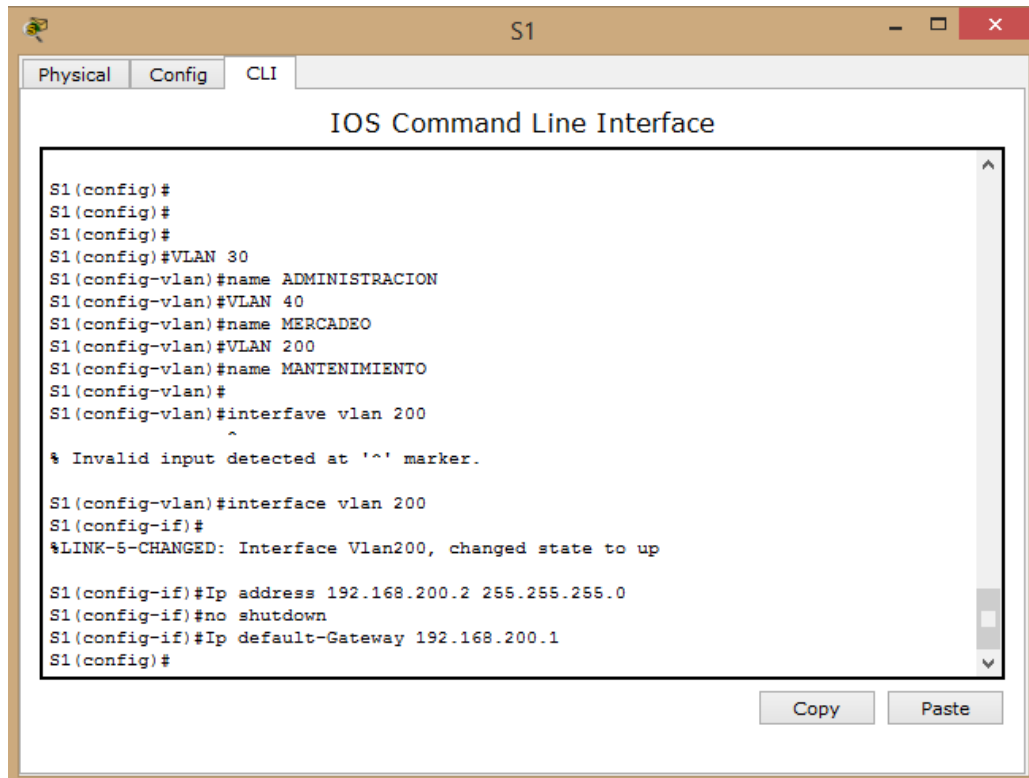
VLAN 30  
Name ADMINISTRACION

VLAN 40  
Name MERCADEO

VLAN 200  
Name MANTENIMIENTO

- Asignar la dirección IP a la Vlan MANTENIMIENTO

Interface VLAN 200  
Ip address 192.168.200.2 255.255.255.0  
No shutdown  
Ip default-Gateway 192.168.200.1



```
S1
Physical Config CLI
IOS Command Line Interface

S1(config)#
S1(config)#
S1(config)#
S1(config)#VLAN 30
S1(config-vlan)#name ADMINISTRACION
S1(config-vlan)#VLAN 40
S1(config-vlan)#name MERCADEO
S1(config-vlan)#VLAN 200
S1(config-vlan)#name MANTENIMIENTO
S1(config-vlan)#
S1(config-vlan)#interface vlan 200
^
% Invalid input detected at '^' marker.

S1(config-vlan)#interface vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

S1(config-if)#Ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#Ip default-Gateway 192.168.200.1
S1(config)#
```



- Forzamos el tranking en la interface f0/3, usamos la vlan nativa 1

Interface **f0/3**

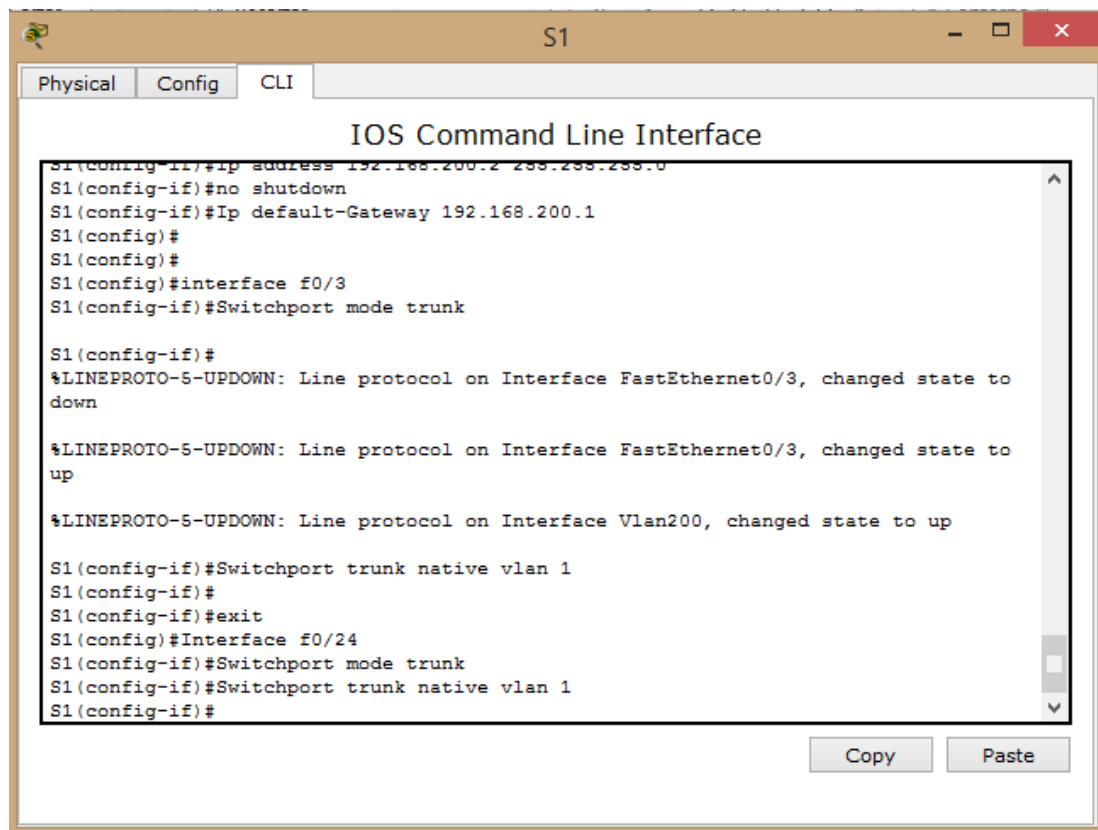
Switchport mode trunk

Switchport trunk native vlan 1

Interface **f0/24**

Switchport mode trunk

Switchport trunk native vlan 1



```
S1(Config-If)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#Ip default-gateway 192.168.200.1
S1(config)#
S1(config)#
S1(config)#interface f0/3
S1(config-if)#Switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S1(config-if)#Switchport trunk native vlan 1
S1(config-if)#
S1(config-if)#exit
S1(config)#Interface f0/24
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 1
S1(config-if)#
```

- Configuramos todos los demás puertos como puertos de acceso.

Interface range fa0/2, fa0/4-23, g0/1-2

Switchport mode Access

Interface **fa0/1**

Switchport mode Access

Switchport Access VLAN 30

- Apagamos los puertos que no los estemos utilizando

Interface range fa0/2, fa0/4-23, g0/1-2  
Shutdown

- Configuramos el S3

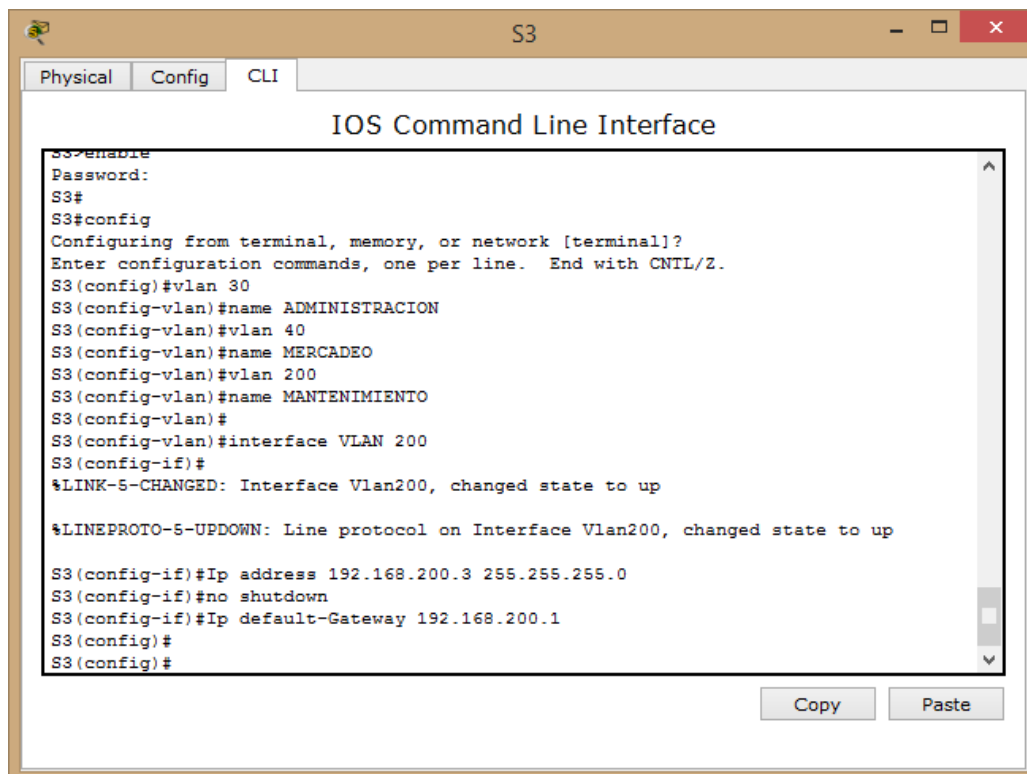
VLAN 30  
Name ADMINISTRACION

VLAN 40  
Name MERCADEO

VLAN 200  
Name MANTENIMIENTO

-

Interface VLAN 200  
Ip address 192.168.200.3 255.255.255.0  
No shutdown  
exit  
Ip default-Gateway 192.168.200.1



- Usamos la f0/3 como troncal y la vlan 1 como nativa

Interface fa0/3

Switchport mode trunk

Switchport trunk native vlan 1

- Configuramos las interfaces en modo acceso empleando el comando rango

Interface range fa0/2, fa0/4-24, g1/1-2

Switchport mode Access

- Asignamos la interface fa0/1 a la vlan 40

Interface fa0/1

Switchport mode access

Switchport Access VLAN 40

- Apagar todos los puertos que no utilicemos

Interface range fa0/2, fa0/4-24, g0/1-2

Shutdown



ip address 192.168.30.1 255.255.255.0

interface g0/0.40

description MERCADEO LAN

encapsulation dot1q 40

ip address 192.168.40.1 255.255.255.0

interface g0/0.200

description MANTENIMIENTO LAN

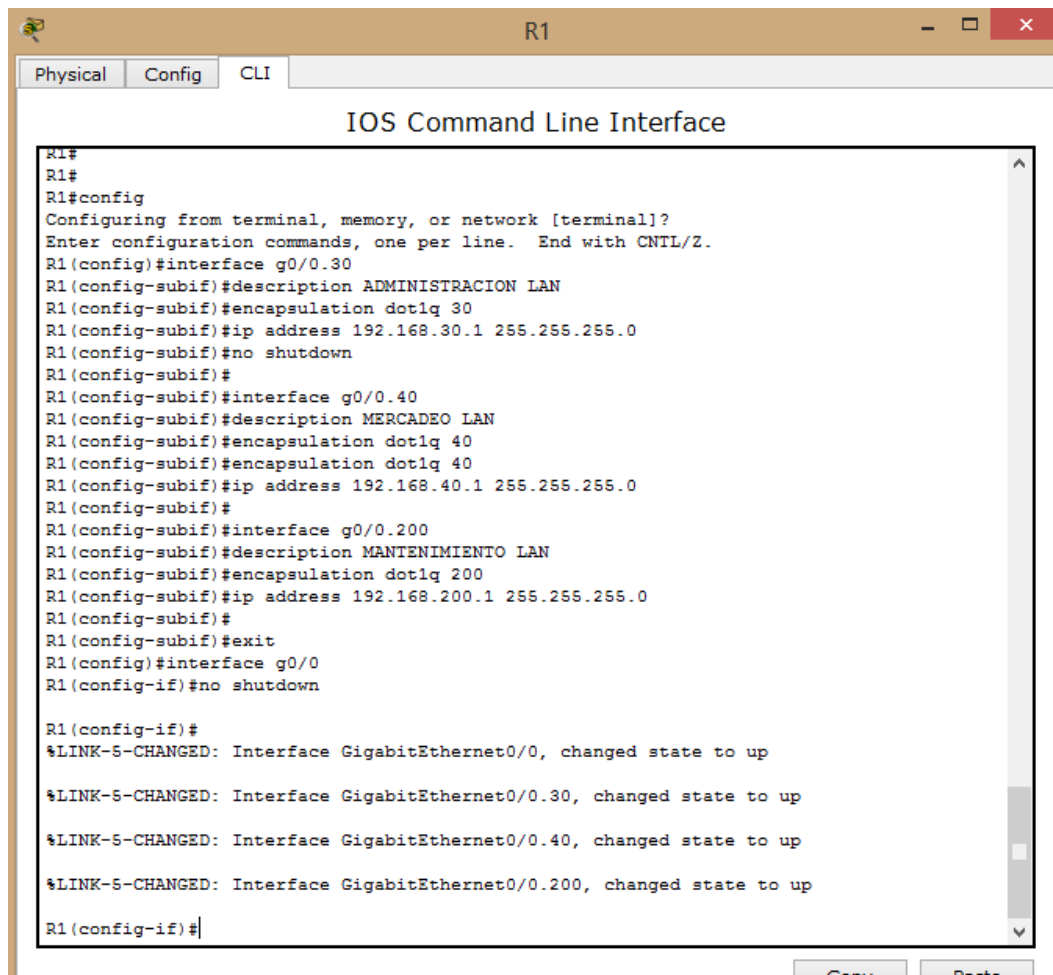
encapsulation dot1q 200

ip address 192.168.200.1 255.255.255.0

- Activamos ahora la interface física g0/0

Interface g0/0

No shutdown



```
R1#
R1#
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0.30
R1(config-subif)#description ADMINISTRACION LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface g0/0.40
R1(config-subif)#description MERCADEO LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#interface g0/0.200
R1(config-subif)#description MANTENIMIENTO LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#exit
R1(config)#interface g0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.200, changed state to up

R1(config-if)#
```

- Procedemos a verificar la conectividad de la red empleando el comando PING

From	To	IP Address	Ping Results
S1	R1, VLAN 99 address		
S3	R1, VLAN 99 address		
S1	R1, VLAN 31 address		
S3	R1, VLAN 33 address		

Todos estos comandos deben ser satisfactorios

S1

Ping 192.168.200.1

Ping 192.168.30.1

```

S1
S1#
S1#
S1#
S1#
S1#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

S1#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

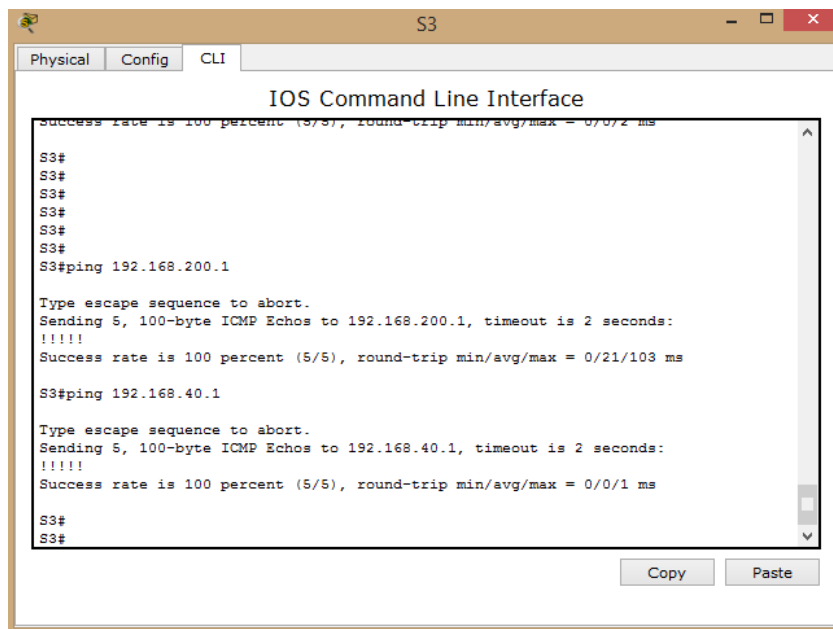
S1#
S1#

```

S3

Ping 192.168.200.1

Ping 192.168.40.1



- Procedemos a configurar OSPF V2 en el router R1

Router ospf 1

Router-id 1.1.1.1

Network 172.31.21.0 0.0.0.3 area 0

Network 192.168.30.0 0.0.0.255 area 0

Network 192.168.40.0 0.0.0.255 area 0

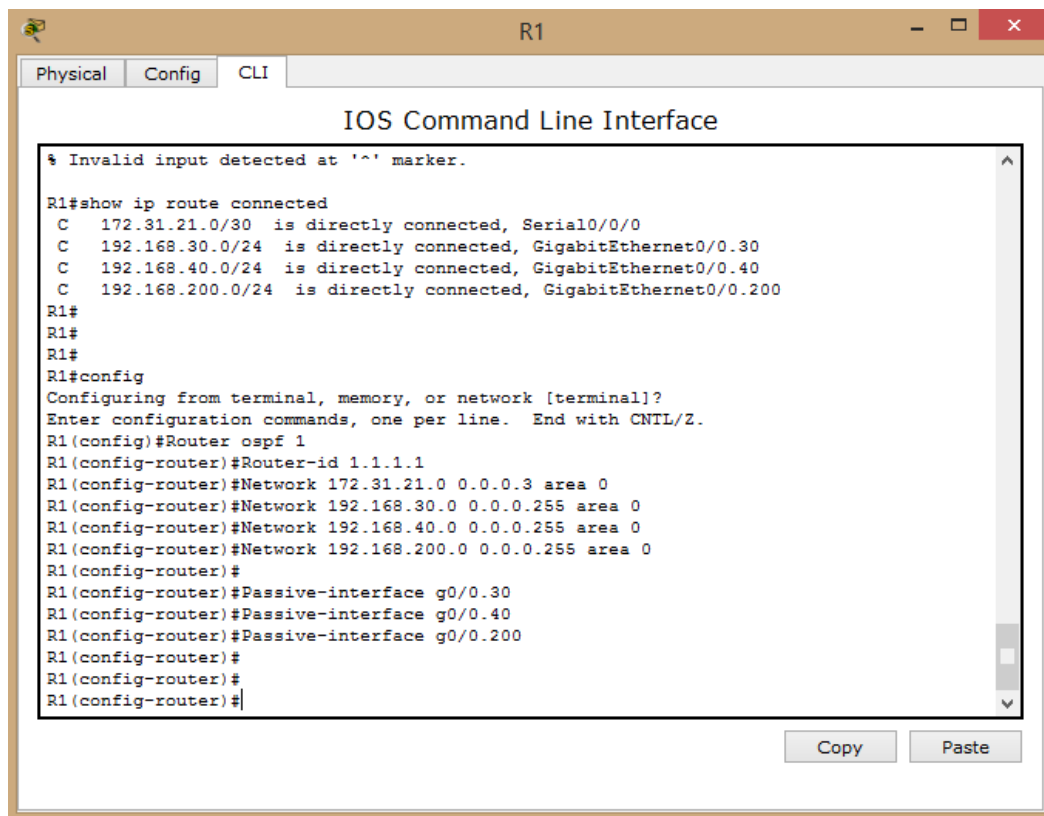
Network 192.168.200.0 0.0.0.255 area 0

- Establecemos todas las interfaces LAN como pasivas

Passive-interface g0/0.30

Passive-interface g0/0.40

Passive-interface g0/0.200



- Cambiamos el costo por defecto

Auto-cost reference-bandwidth 1000 “este comando no es soportado por el simulador”

- Cambiamos el ancho de banda de las interfaces seriales

Interface s0/0/0  
Bandwidth 128  
Ip ospf cost 7500

- Configuramos OPSF V2 en el router R2

Router ospf 1  
Router-id 2.2.2.2  
Network 172.31.21.0 0.0.0.3 area 0  
Network 172.31.23.0 0.0.0.3 area 0  
Network 10.10.10.0 0.0.0.255 area 0

- Establecemos las LAN como pasivas



Passive-interface g0/0

Interface s0/0/0

Bandwidth 128

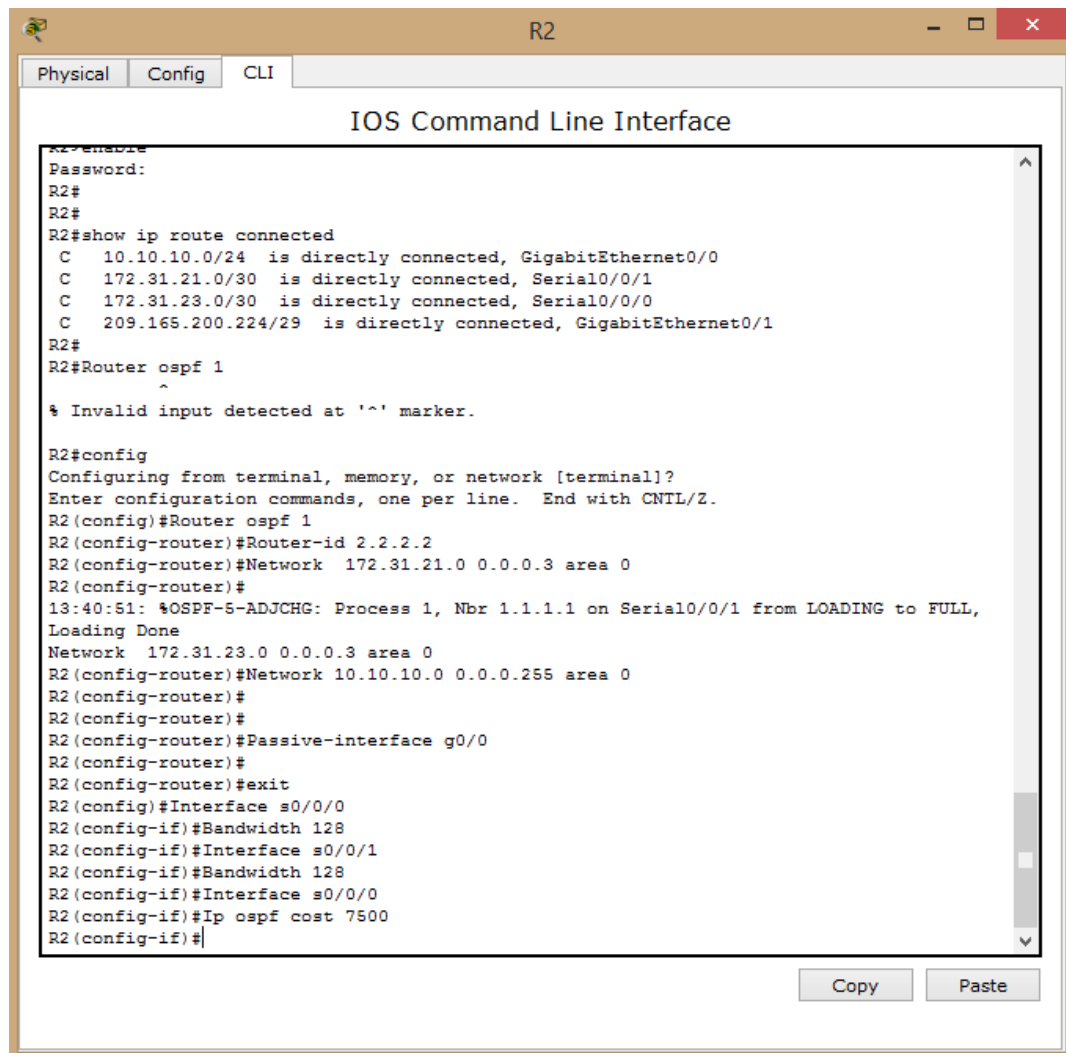
Interface s0/0/1

Bandwidth 128

Ajustar la métrica de serial s0/0/0

Interface s0/0/0

Ip ospf cost 7500



```
R2
Physical Config CLI
IOS Command Line Interface
R2>enable
Password:
R2#
R2#
R2#show ip route connected
C 10.10.10.0/24 is directly connected, GigabitEthernet0/0
C 172.31.21.0/30 is directly connected, Serial0/0/1
C 172.31.23.0/30 is directly connected, Serial0/0/0
C 209.165.200.224/29 is directly connected, GigabitEthernet0/1
R2#
R2#Router ospf 1
^
% Invalid input detected at '^' marker.

R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Router ospf 1
R2(config-router)#Router-id 2.2.2.2
R2(config-router)#Network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
13:40:51: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-router)#Network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#Network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#
R2(config-router)#
R2(config-router)#Passive-interface g0/0
R2(config-router)#
R2(config-router)#exit
R2(config)#Interface s0/0/0
R2(config-if)#Bandwidth 128
R2(config-if)#Interface s0/0/1
R2(config-if)#Bandwidth 128
R2(config-if)#Interface s0/0/0
R2(config-if)#Ip ospf cost 7500
R2(config-if)#
```

- Configuramos OPSF V2 en el router R3

Router ospf 1

Router-id 3.3.3.3

Network 172.31.23.0 0.0.0.3 area 0

Network 192.168.4.0 0.0.3.255 area 0

- Debemos hacer que todas las interfaces loopback sean pasivas

Passive-interface lo4

Passive-interface lo5

Passive-interface lo6

Interface s0/0/1

Bandwidth 128

```
R3#
R3#
R3#show ip route connected
C 172.31.23.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3#
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#Router ospf 1
R3(config-router)#Router-id 3.3.3.3
R3(config-router)#Network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#Network 922.168.4.0 0.0.3.255 area 0
^
% Invalid input detected at '^' marker.

R3(config-router)#
13:45:27: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
FULL, Loading Done

R3(config-router)#Network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#Passive-interface lo4
R3(config-router)#Passive-interface lo5
R3(config-router)#Passive-interface lo6
R3(config-router)#exit
R3(config)#Interface s0/0/1
^
% Invalid input detected at '^' marker.

R3(config)#Interface s0/0/1
R3(config-if)#Bandwidth 128
R3(config-if)#
```

- Debemos verificar los comandos OSPF.

- Show ip ospf neighbor
- Show ip protocols
- Show ip route ospf
- Do show ip route connected

- Show ip ospf neighbor

R2#Show ip ospf neighbor

Neighbor ID	Pri	State		Dead Time	Address	Interface
1.1.1.1	0	FULL/	-	00:00:32	172.31.21.1	Serial0/0/1
3.3.3.3	0	FULL/	-	00:00:36	172.31.23.2	Serial0/0/0

R2#

R1#show ip ospf neighbor

Neighbor ID	Pri	State		Dead Time	Address	Interface
2.2.2.2	0	FULL/	-	00:00:31	172.31.21.2	Serial0/0/0

R1#  
R1#

R3#Show ip ospf neighbor

Neighbor ID	Pri	State		Dead Time	Address	Interface
2.2.2.2	0	FULL/	-	00:00:36	172.31.23.1	Serial0/0/1

R3#

- Show ip route ospf

R3#Show ip route ospf

```
10.0.0.0/24 is subnetted, 1 subnets
O    10.10.10.0 [110/782] via 172.31.23.1, 00:04:08, Serial0/0/1
172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O    172.31.21.0 [110/1562] via 172.31.23.1, 00:04:08, Serial0/0/1
O    192.168.30.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
O    192.168.40.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
O    192.168.200.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
R3#
```

R2#Show ip route ospf

```
192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.1 [110/7501] via 172.31.23.2, 00:05:09, Serial0/0/0
192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.1 [110/7501] via 172.31.23.2, 00:04:59, Serial0/0/0
192.168.6.0/32 is subnetted, 1 subnets
O    192.168.6.1 [110/7501] via 172.31.23.2, 00:04:59, Serial0/0/0
O    192.168.30.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
O    192.168.40.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
O    192.168.200.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
R2#
R2#
```

```

R1#Show ip route ospf
    10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0 [110/7501] via 172.31.21.2, 00:10:38, Serial0/0/0
    172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.23.0 [110/15000] via 172.31.21.2, 00:08:56, Serial0/0/0
    192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/15001] via 172.31.21.2, 00:05:32, Serial0/0/0
    192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/15001] via 172.31.21.2, 00:05:22, Serial0/0/0
    192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/15001] via 172.31.21.2, 00:05:22, Serial0/0/0
R1#
R1#

```

- Comando para verificar la configuración en ejecución

- show running-config

- Debemos implementar DHCP en el router R1.

- Procedemos en este caso a reservar las 30 primaras direcciones, tanto de la VLAN 30 como la VLAN 40.

Ip dhcp excluded-address 192.168.30.1 192.168.30.30

Ip dhcp excluded-address 192.168.40.1 192.168.40.30

Ip dhcp pool ADMINISTRACION

Dns-server 10.10.10.11

Domain-name ccna-unad.com

“comando no soportado”

Default-router 192.168.30.1

Network 192.168.30.0 255.255.255.0

Ip dhcp pool MERCADEO

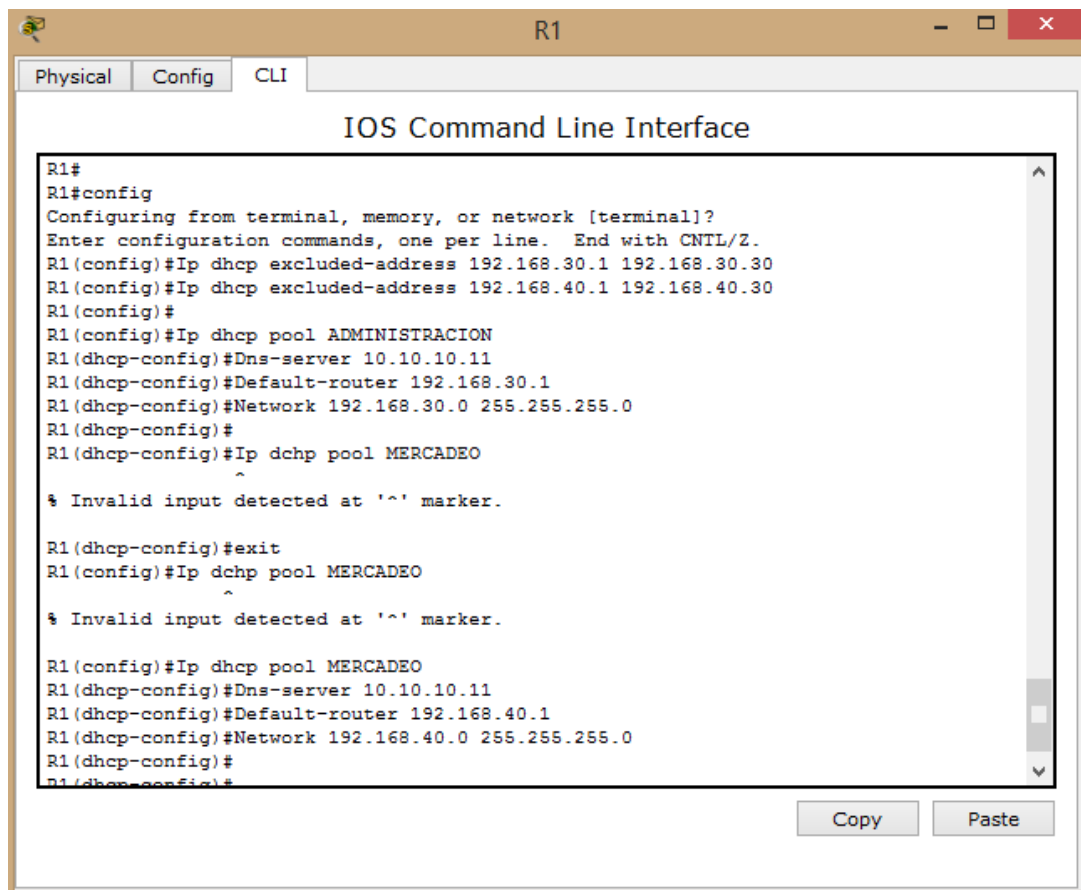
Dns-server 10.10.10.11

Domain-name ccna-unad.com

“comando no soportado”

Default-router 192.168.40.1

Network 192.168.40.0 255.255.255.0



The screenshot shows a terminal window titled 'R1' with tabs for 'Physical', 'Config', and 'CLI'. The main window displays the 'IOS Command Line Interface' with the following commands and output:

```
R1#
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#Ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#
R1(config)#Ip dhcp pool ADMINISTRACION
R1(dhcp-config)#Dns-server 10.10.10.11
R1(dhcp-config)#Default-router 192.168.30.1
R1(dhcp-config)#Network 192.168.30.0 255.255.255.0
R1(dhcp-config)#
R1(dhcp-config)#Ip dhcp pool MERCADEO
^
% Invalid input detected at '^' marker.

R1(dhcp-config)#exit
R1(config)#Ip dhcp pool MERCADEO
^
% Invalid input detected at '^' marker.

R1(config)#Ip dhcp pool MERCADEO
R1(dhcp-config)#Dns-server 10.10.10.11
R1(dhcp-config)#Default-router 192.168.40.1
R1(dhcp-config)#Network 192.168.40.0 255.255.255.0
R1(dhcp-config)#
R1(dhcp-config)#
```

At the bottom right of the terminal window, there are 'Copy' and 'Paste' buttons.

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

- Configuramos NAT ESTATICO y DINAMICO en R2 con el fin de que los hosts puedan salir a internet.

## Step 2: Configure Static and Dynamic NAT on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification
Create a local database with 1 user account	Username: <b>webuser</b> Password: <b>cisco12345</b> Privilege level: <b>15</b>
Enable HTTP server service	
Configure the HTTP server to use the local database for authentication	
Create a static NAT to the Web Server	Inside Global Address: <b>209.165.200.229</b>
Assign the inside and outside interface for the static NAT	
Configure the dynamic NAT inside private ACL	Access List: 1 Allow the Accounting and Engineering networks of R1 to be translated. Allow a summary of the LANs (loopback) networks on R3 to be translated.
Define the pool of usable public IP addresses	Pool Name: <b>INTERNET</b> Pool of addresses include: <b>209.165.200.225 – 209.165.200.228</b>
Define the dynamic NAT translation	

User webuser privilege 15 secret cisco12345

- En este caso debemos usar el servidor web.

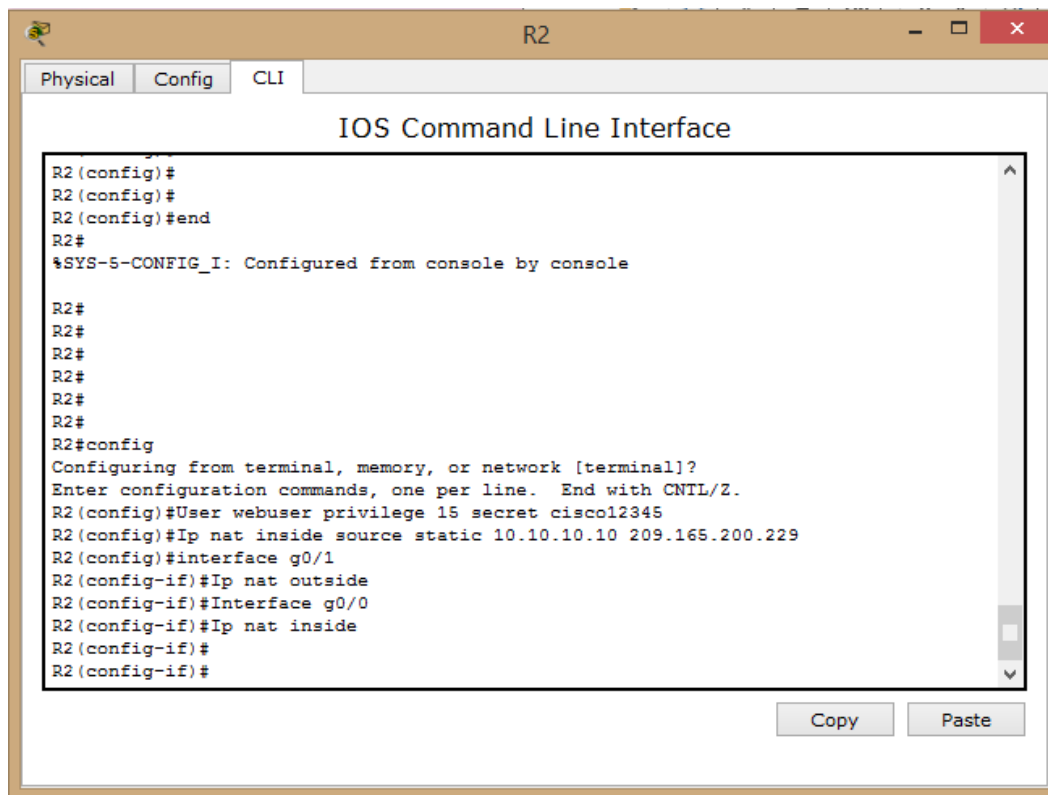
Ip nat inside source static 10.10.10.10 209.165.200.229

- Asignamos la interface interna y externa



Interface g0/1  
Ip nat outside

Interface g0/0  
Ip nat inside



- Creamos algunas restricciones empleando las ACL.
- Configuramos la NAT DINAMICA con una ACL.
- Creamos la acces-list número 1
- Solo debemos permitir que la traducción sea para las redes de ADMINISTRACIÓN Y MERCADEO que están en R1 – pero la traducción se hace en R2.

Configure terminal

Access-list 1 permit 192.168.30.0 0.0.0.255

Access-list 1 permit 192.168.40.0 0.0.0.255

- Permitir que las loopback que están conectadas al R3 también sean traducidas empleando una ruta RESUMIDA.

Access-list 1 permit 192.168.4.0 0.0.3.255

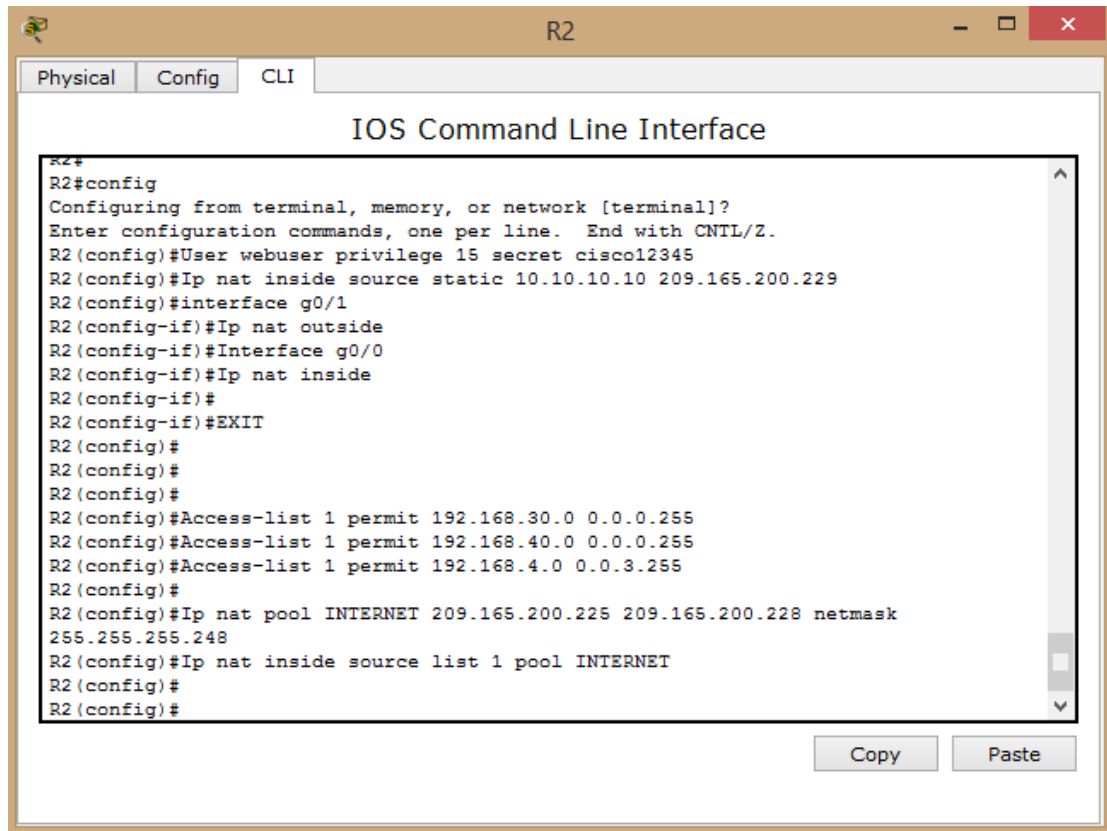
- Definimos el POOL de direcciones que se van a utilizar para el NAT DINAMICO.



Ip nat pool **INTERNET** 209.165.200.225 209.165.200.228 netmask 255.255.255.248

- Definimos la traducción NAT dinámico

Ip nat inside source list 1 pool INTERNET



The screenshot shows a window titled "R2" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and prompts:

```
R2#
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#User webuser privilege 15 secret cisco12345
R2(config)#Ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface g0/1
R2(config-if)#Ip nat outside
R2(config-if)#Interface g0/0
R2(config-if)#Ip nat inside
R2(config-if)#
R2(config-if)#EXIT
R2(config)#
R2(config)#
R2(config)#
R2(config)#Access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#
R2(config)#Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#Ip nat inside source list 1 pool INTERNET
R2(config)#
R2(config)#
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

- Procedemos a verificar lo hecho hasta este momento.

### Step 3: Verify DHCP and Static NAT.

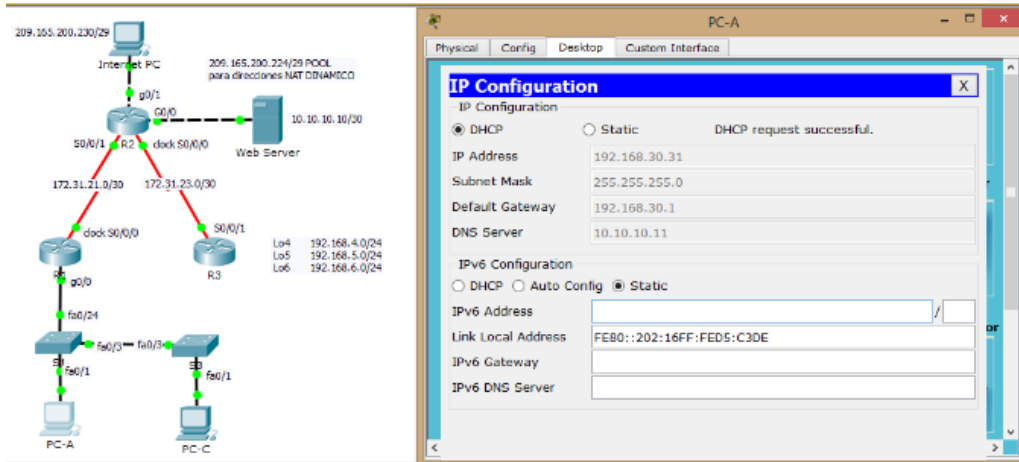
Use the following tasks to verify that DHCP and Static NAT settings are functioning correctly. If necessary to disable the PC firewall for pings to be successful:

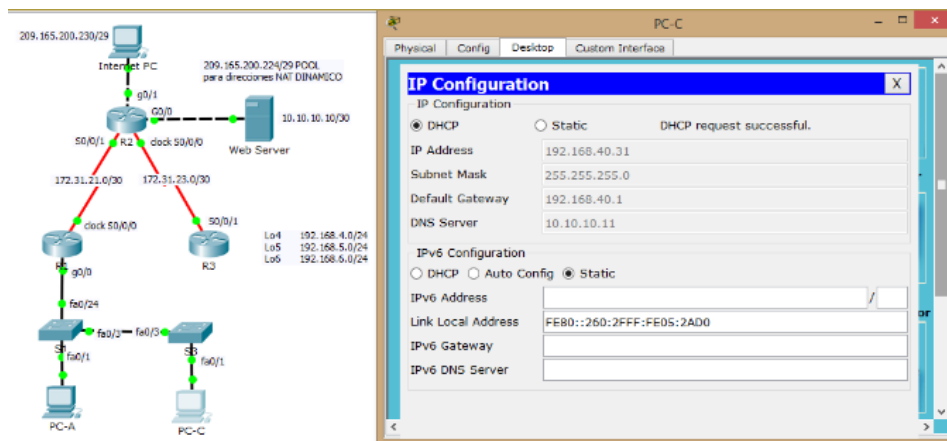
Test	Results
Verify that PC-A acquired IP information from the DHCP server	
Verify that PC-C acquired IP information from the DHCP server	
Verify that PC-A can ping PC-C. <b>Note:</b> It may be necessary to disable the PC firewall	
Use a Web browser on the Internet PC to access the Web server (209.165.200.229). Login with Username: <b>webuser</b> , Password: <b>cisco12345</b>	

**Note:** Verification of dynamic NAT will be performed in Part 6.

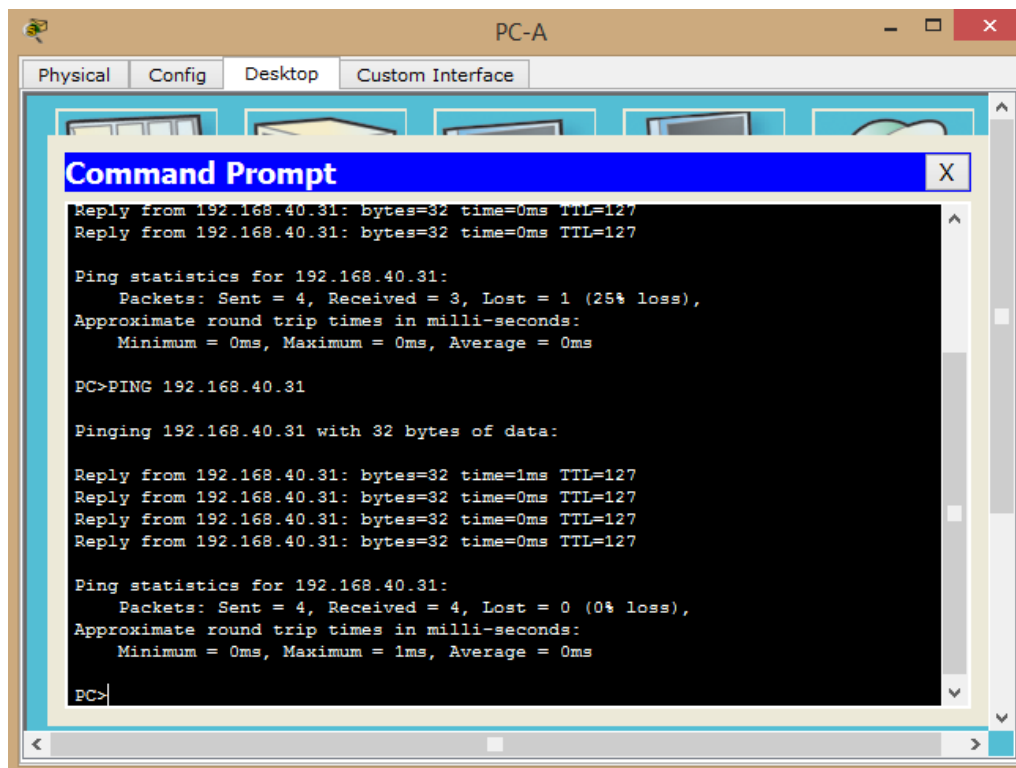
**Instructor Sign-off Part 2:** \_\_\_\_\_

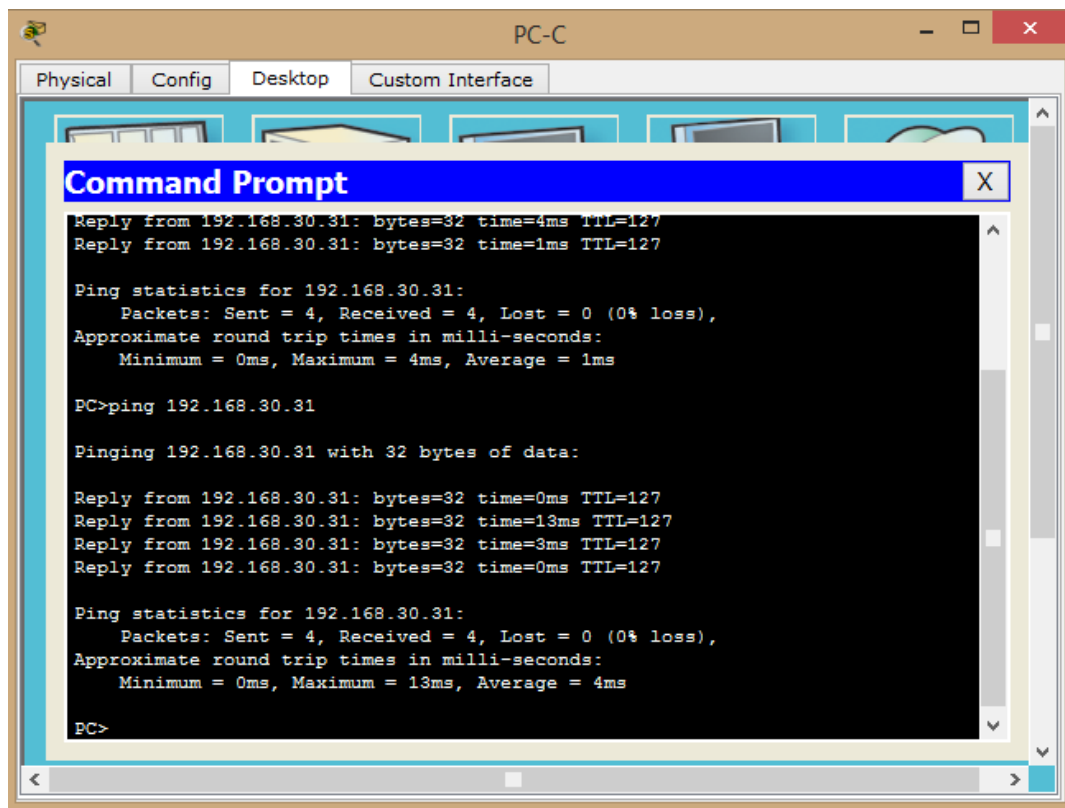
Points: \_\_\_\_\_ of 13





- Ping entre PC-A y PC-C





- Configurar y verificar las ACL en el router R2 en la cual solo le damos acceso al router R1.

- Configuramos una ACL que me permita que solo R1 pueda hacer TELNET a R2.

Ip Access-list standard **ADMIN-MANTENIMIENTO**  
Permit host 172.31.21.1

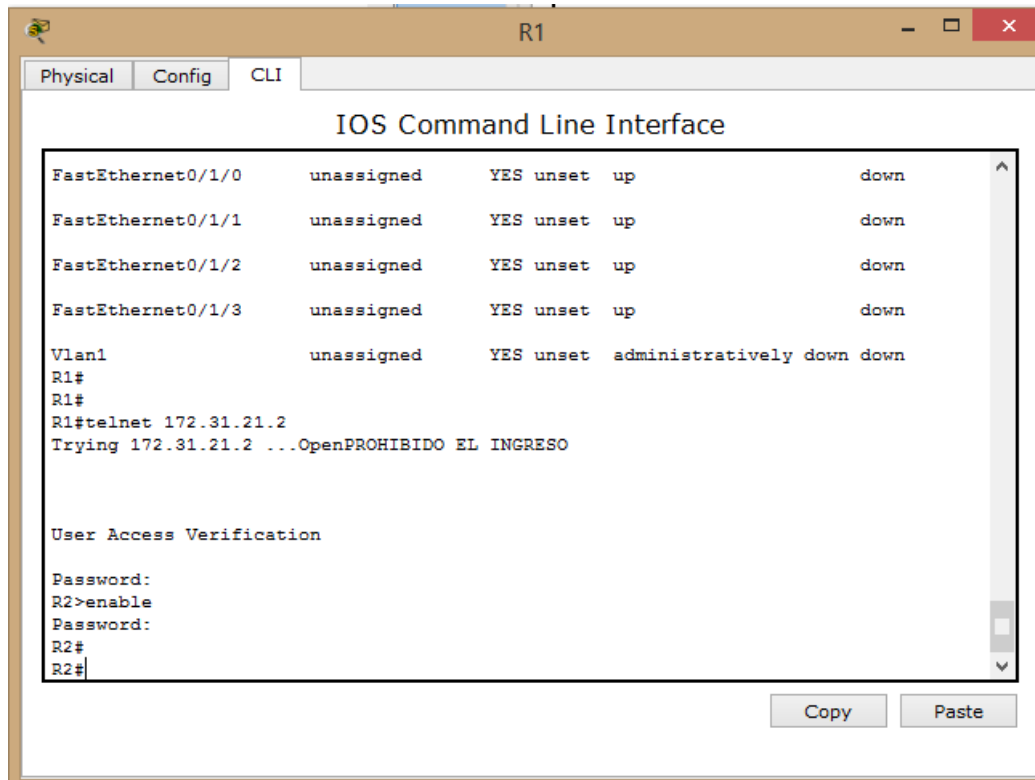
- Ahora si debemos aplicar la ACL nombrada a la línea VTY

Line vty 0 4  
Access-class **ADMIN-MANTENIMIENTO** in

- Debemos verificar que las ACL está trabajando como queremos

Vemos claramente que si empleamos TELNET desde el ROUTER R1 este es satisfactorio, si lo hacemos desde cualquier otro equipo este no puede ser posible.

- Si hacemos TELNET al router R2 desde el router R1 este es SATISFACTORIO, tal como lo indica nuestra ACL.



- Si hacemos TELNET desde un equipo de cualquiera de las VLAN.

```

PC>
PC>
PC>telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
PC>
PC>
  
```

- Si hacemos TELNET desde R3.

```

R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
R3#
R3#
R3#
R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
R3#

```

- Aseguramos la red del tráfico de INTERNET, de este modo estas no son posibles.

Configuration Item or Task	Specification
<b>Configure an Extended ACL to:</b> <ul style="list-style-type: none"> <li>• Allow Internet hosts WWW access to the simulated web server on R2 by accessing the static NAT address (209.165.200.229) that you configured in Part 3.</li> <li>• Prevent traffic from the Internet from pinging internal networks, while continuing to allow LAN interfaces to ping the Internet PC.</li> </ul>	ACL No.: <b>101</b>
Apply ACL to the appropriate interface(s)	
Verify ACL is working as expected	From the Internet PC: <ul style="list-style-type: none"> <li>• Ping PC-A (Pings should be unreachable.)</li> <li>• Ping PC-C (Pings should be unreachable.)</li> </ul> From R1, Ping the Internet PC (Pings should be successful.)

### • En R2

Access-list **101** permit tcp any host **209.165.229.230** eq www

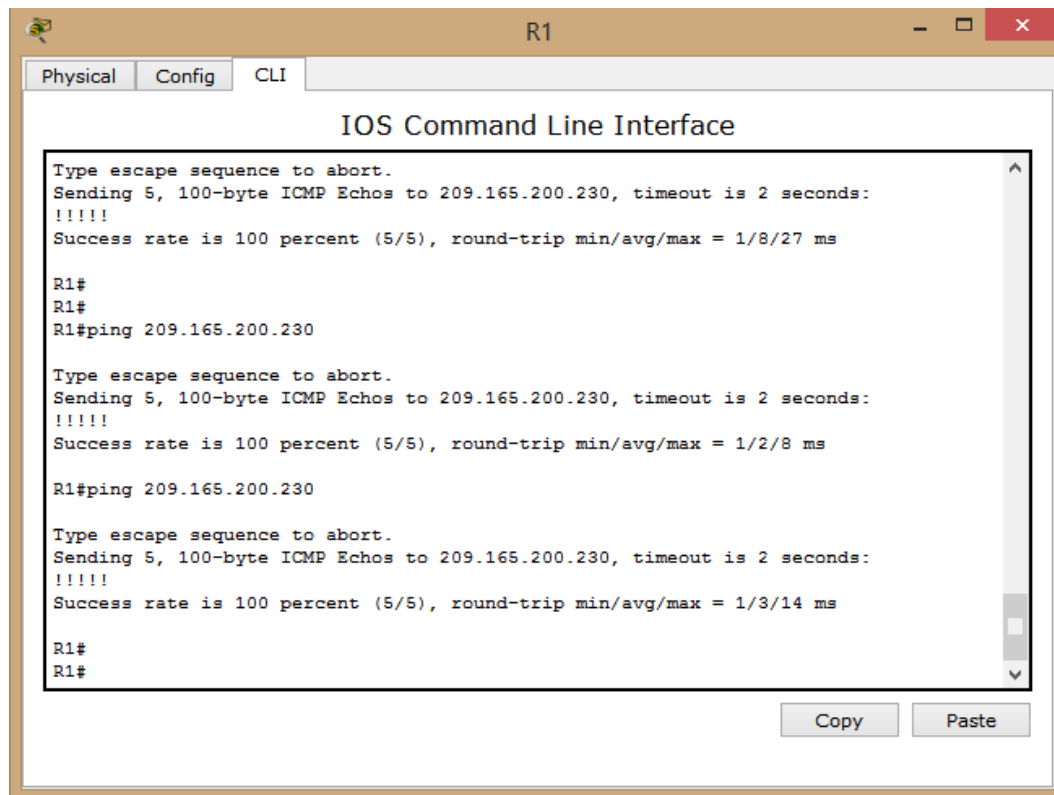
- Prevenir el tráfico desde INTERNET que no puedan hacer PING a la red interna

Access-list **101** permit icmp any any echo-reply

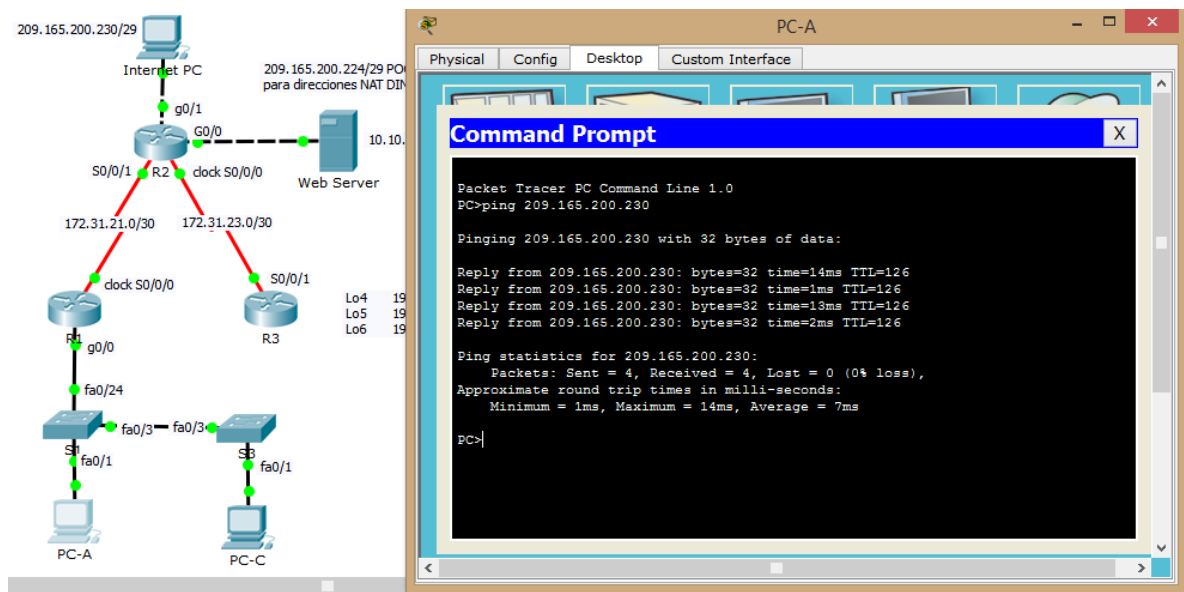
- Debemos aplicar las ACL a las interfaces adecuadas.

```
Interface g0/1
Ip Access-group 101 in
Interface s0/0/0
Ip Access-group 101 out
Interface s0/0/1
Ip Access-group 101 out
Interface g0/0
Ip Access-group 101 out
```

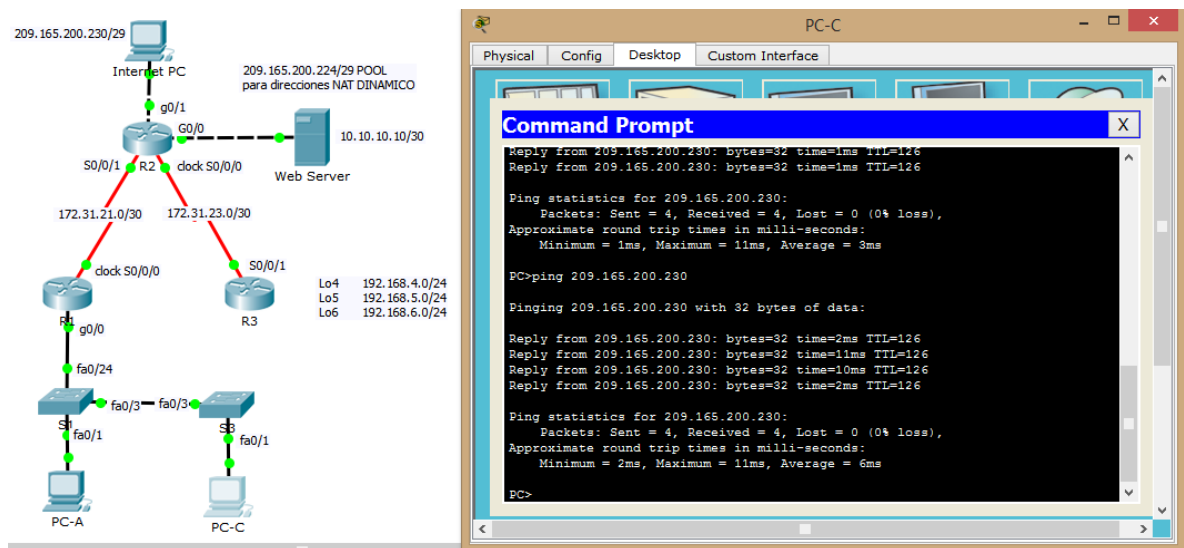
- Procedemos a verificar que las ACL están funcionando



- Vamos a realizar el mismo proceso, pero en este CASO desde los PC de las VLAN.
- Desde la PC-A

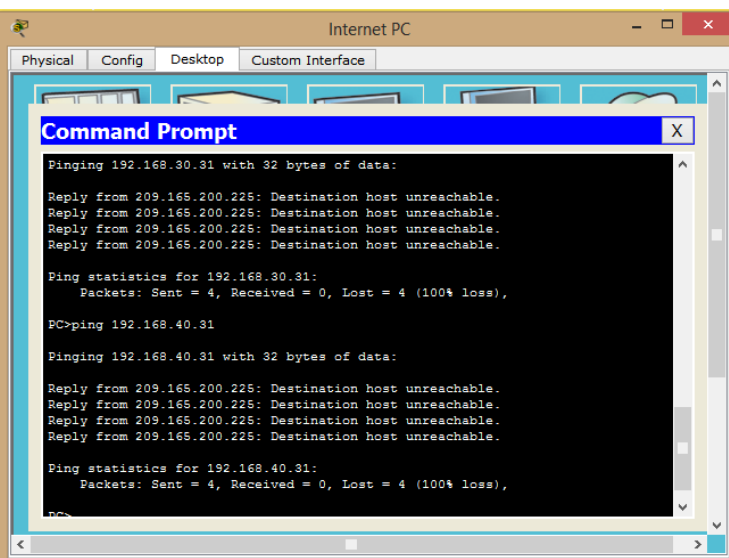
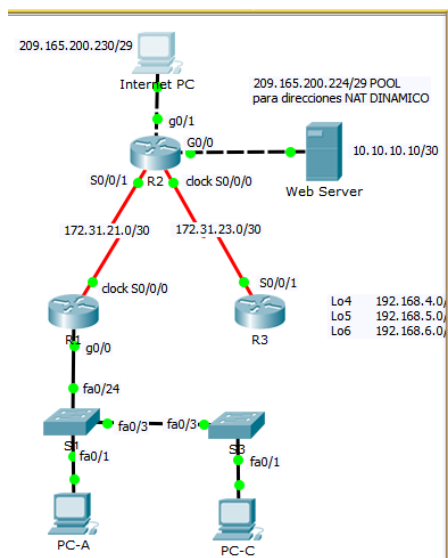


- Desde la PC-C



- PING desde PC INTERNET hacia la PC-A y la PC-C





## CONCLUSIONES

- Lo importante para desarrollar confianza en nosotros para en la implementación de este tipo de propuestas es practicar mucho.
- Cada vez más debemos fortalecer nuestros conocimientos profundizando constantemente en los cambios que cada uno de ellos ha tenido.
- En todo el diseño de la red aplicamos VLSM gracias al cual el desperdicio de direcciones IP es mínimo y ajustado realmente a las necesidades Ip de cada una de las subredes.
- Bueno, definitivamente todo lo trabajado y el material didáctico utilizado en el transcurso del diplomado han sido de vital importancia para llegar donde estamos, todo lo hemos utilizado en este punto del curso, los cuadros, los comandos, etc.
- El diseño que realice para la empresa funciona a la perfección, se realizaron todas las pruebas de caso y todas arrojan resultado favorable.
- La vida que tenemos está muy relacionada con la tecnología, esta ocupa parte fundamental dentro de nuestras vidas tanto familiares como laborales.
- Ya no tenemos barreras ni de tiempo ni mucho menos de espacio, podemos acceder a los que queramos en el lugar donde se encuentre.
- Veo con mucha seguridad que el Diplomado me ha aportado mucho para mi vida laboral.
- Veo que la temática desarrollada ha ayudado a mi formación integral.
- He desarrollado este proyecto desde cero y me agrada el grado de conocimiento que tengo relacionado a los dispositivos y su configuración.

## **BIBLIOGRAFÍA**

- Cisco Networking Academy. <https://www.netacad.com/es>